

All-Optical Quantum Random Bit Generation from Intrinsically Binary Phase of Parametric Oscillators

Alireza Marandi*, Nick C. Leindecker, Konstantin L. Vodopyanov, and Robert L. Byer

E. L. Ginzton Laboratory, Stanford University, CA 94305,

marandi@stanford.edu

March 6, 2013

True random number generators (RNGs) are desirable for applications ranging from cryptography to computer simulations. Quantum phenomena prove to be attractive for physical RNGs due to their fundamental randomness and immunity to attack [1]– [5]. Optical parametric down conversion is an essential element in most quantum optical experiments including optical squeezing [9], and generation of entangled photons [10]. In an optical parametric oscillator (OPO), photons generated through spontaneous down conversion of the pump initiate the oscillation in the absence of other inputs [11, 12]. This quantum process is the dominant effect during the oscillation build-up, leading to selection of one of the two possible phase states above threshold in a degenerate OPO [13]. Building on this, we demonstrate a novel all-optical quantum RNG in which the photodetection is not a part of the random process, and no post processing is required for the generated bit sequence. We implement a synchronously pumped twin degenerate OPO, which comprises two identical independent OPOs in a single cavity, and measure the relative phase states of the OPO outputs above threshold as a bit value. We show that the outcome is statistically random with 99% confidence. With the use of micro- and nanoscale OPO resonators, this technique offers a promise for simple, robust, and high-speed on-chip all-optical quantum random number generators.

Intrinsic randomness in quantum theory has led to RNG proposals based on the measurement of quantum observables. It was recently demonstrated that quantum correlation of non-local states in two entangled atomic systems can violate Bell inequality principle and be used to generate random numbers [1]. Entangled-photon and single-photon sources have been used for RNGs [2]. Phase of vacuum fluctuations measured by a homodyne detection scheme [3], photon arrival time [4], and randomness in photon number distribution of a coherent source [5] have also been exploited as the engines of RNGs. Some other quantum RNGs are based on phase measurements of laser diode outputs [6, 7] and the Stokes light in Raman scattering [8]. Most of these methods require massive post-processing to ensure randomness, in some, photodetection is an essential part of the random process, and several require a complicated experimental environment.

The quantum RNG proposed in this letter does not require sophisticated detection techniques because the OPO operates above threshold. Our system is further simplified by using commercially available fiber lasers and well-developed quasi phase matching technology for nonlinear crystals [14]. The optical beam at the output randomly toggles between two intensity levels with a well-defined clock signal. The randomness is intrinsically inherited from the quantum noise of the system, and we verify minimal contribution of classical

noise sources by examining the dependence of randomness on the phase of initiating photons in the OPO. A sequence of 1 billion bits is generated at 10 kbps which has successfully passed all the statistical randomness tests provided by National Institute of Standards and Technology (NIST).

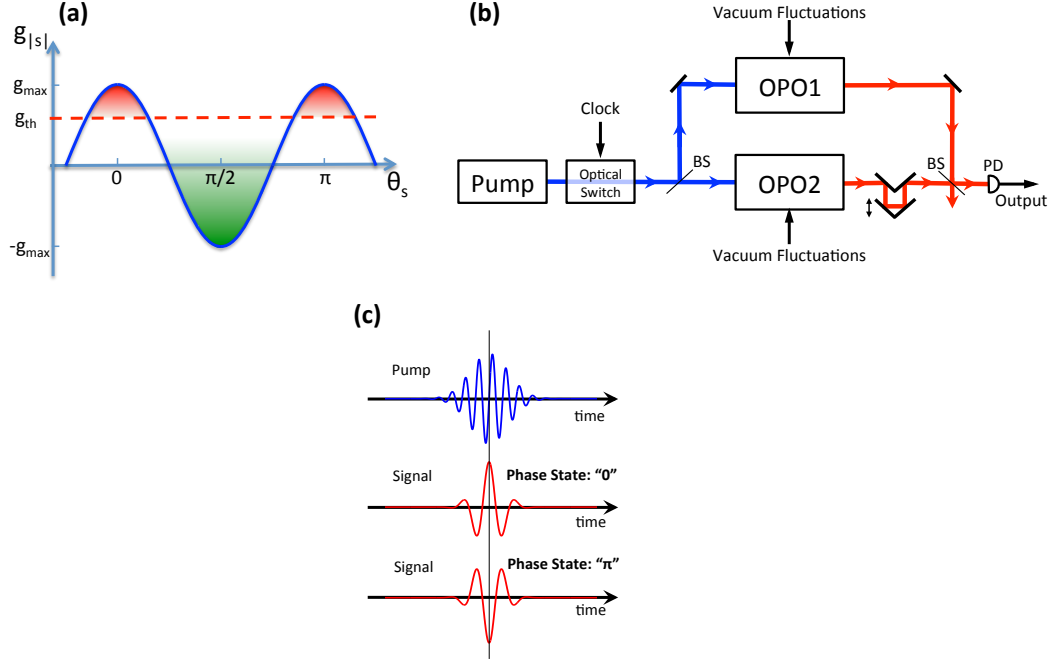


Figure 1: a) Phase sensitive gain in a degenerate OPO – the amplitude incremental gain of the signal ($g_{|s|}$) versus the relative phase between the pump and the signal – ($\theta_s = \phi_s - \phi_p/2 + \pi/4$, where ϕ_s and ϕ_p are the signal and pump phases, respectively), b) Schematic of the all-optical quantum RNG. PD: Photodetector, BS: non-polarizing beam splitter, c) Electric fields of the signal pulses compared to the pump in the two possible phase states of a short-pulse degenerate OPO.

The operation principle is based on the phase response of a degenerate OPO. In a continuous wave (c.w.) type I degenerate OPO, where signal and idler are indistinguishable (we call it signal in this letter), stable oscillation above threshold can occur in one of the two possible phase states [13]. This is because the gain mechanism in such an OPO, provided by degenerate parametric amplification, is phase sensitive and has a period of π for the signal phase [15]. Figure 1-(a) schematically illustrates the incremental amplitude gain in such an amplifier as a function of the relative phase between the pump and the signal (θ_s). Maximum amplification occurs both at $\theta_s = 0$ and $\theta_s = \pi$, where the energy flows from the pump into the signal, and maximum deamplification at $\theta_s = \pi/2$ where the energy flow is from the signal to the pump. Equivalently, this period of π exists in the phase dependence of quantum fluctuations in a squeezed state produced by degenerate parametric down conversion [9]. If the maximum gain exceeds the loss in the resonator ($g_{max} > g_{th} = \delta_E$, where δ_E is the electric field round-trip loss [15]), depending on the zero-point fluctuations of the signal modes, the OPO will stably oscillate with the phase of either $\theta_s = 0$ or $\theta_s = \pi$. This above-threshold phase state is inherited from the vacuum fluctuations [9], and none of the design parameters favors oscillation in one or another.

To make a quantum RNG based on this process, the relative phase states between two identical OPOs can be measured by interfering the outputs. This is demonstrated in the schematic in Fig. 1-(b), where two degenerate OPOs are pumped with the same source, and an optical switch is used to restart the OPOs periodically. If both path lengths are matched, the interference of the output signals will randomly toggle between high and low intensity levels resulting in a sequence of “zeros” and “ones” at the photodetector output.

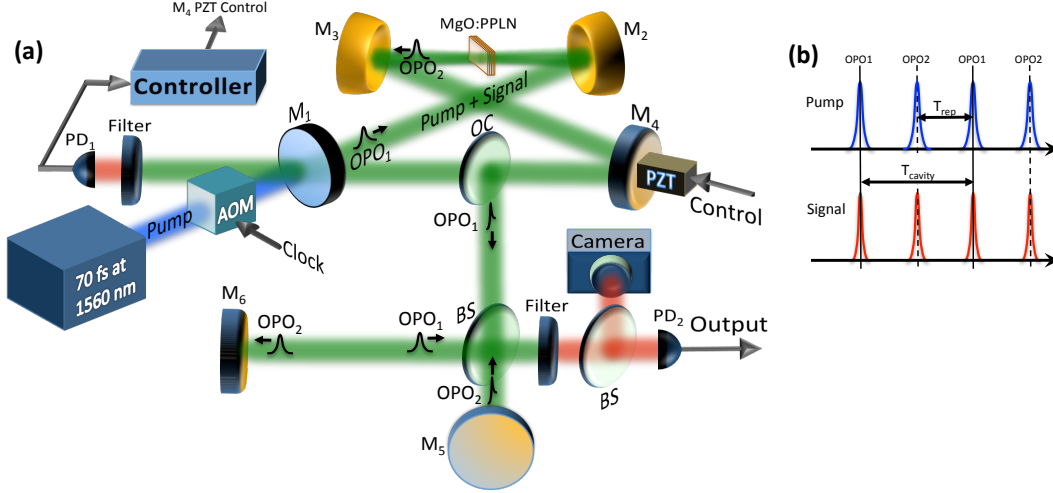


Figure 2: a) Schematic of the experimental setup consisting of the twin degenerate OPO followed by an un-equal arm Michelson interferometer. The round-trip length difference of the arms in the interferometer is equal to the separation length of pump pulses. The output of the interferometer is filtered to eliminate the pump. An AOM is used to restart the twin OPO at a clock rate of 10 kbps, while the zeroth order output (non-diffracted beam) pumps the OPO. The detector PD1 and a piezoelectric transducer (PZT) on M4 are parts of the “dither-and-lock” servo loop for stabilizing the cavity length to a resonance [18]. The interferometer arm length difference is stabilized using the interference of the undepleted pump and a PZT on M6 which is not shown in this schematic. OC: Output Coupler, b) Pump and signal pulse trains for a twin OPO in which the cavity roundtrip time (T_{cavity}) is twice the repetition period of the pump (T_{rep}); this results in two independent OPOs with signal pulse trains at half the repetition frequency of the pump, marked by OPO1 and OPO2 on the pulse trains.

We realized the OPO-based quantum RNG using the synchronously pumped femtosecond degenerate OPO demonstrated in [16]. For such a short-pulse OPO, similar to the c.w. case, the signal can take one of the two possible phase states [17] which destructively interfere with each other. Fig. 1-(c) depicts an example of the electric field of the pump and the signal in the two possible phase states. The existence of these phase states for a degenerate femtosecond OPO was experimentally verified in [18].

To avoid implementation of two matched resonators, a twin OPO is used, in which two identical OPOs operate in the same ring resonator with the roundtrip path length twice the separation length of pump pulses, as depicted in Fig. 2-(a). Fig. 2-(b) shows the pump and signal pulse trains for this twin OPO. The pump pulses generate two independent signal pulse trains, marked as OPO1 and OPO2 in the figure. These two temporally separated OPOs have half the repetition rate of the pump, the same polarization and spectral

properties, and experience exactly the same optical paths in the oscillator. An unequal arm interferometer is used to measure the relative phase states of OPO1 and OPO2 by interfering their temporally separated pulse trains, as depicted in the schematic of Fig. 2- (a).

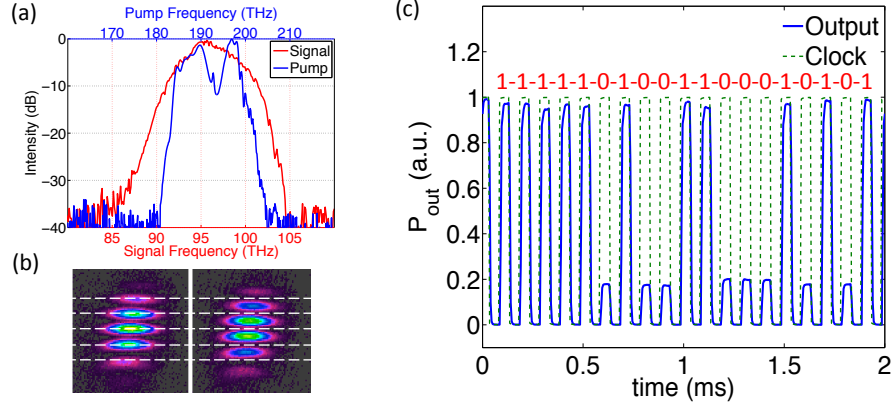


Figure 3: a) Optical spectrum of the pump and signal, b) complementary fringe patterns at the output of the Michelson interferometer, i.e. maximum on one pattern is minimum on the other and vice versa, c) sample time domain signal of the interferometer output, i.e. the random sequence, along with the clock signal at 10 kbps.

The OPO stabilized with the servo loop could run continuously for several days (see Methods). Figure 3-(a) shows the signal spectrum centered at $3.1 \mu\text{m}$ and the pump centered at $1.56 \mu\text{m}$. Complementary stable fringe patterns at the output of the interferometer were obtained as depicted in Fig. 3-(b) when the beams in the arms are slightly angled vertically. Blocking and unblocking the pump resulted in random toggling between these two patterns.

To capture a bit stream, the beam angles are well-aligned in the interferometer and a photodetector is used at the output, while an Acousto-Optic Modulator (AOM) causes periodic restarting of the twin OPO. Figure 3-(c) depicts a sample of the signal at the output of the interferometer along with the clock signal at 10 Kbps applied to the AOM. The binary sequence is extracted from the interferometer output as depicted in the plot.

A sequence of 1 billion bits is taken with this method, and it proves to be random with an average of 0.5000. To verify the statistical randomness, a series of tests developed by NIST [19] are performed, and the summary of results are presented in Fig. 4. The 1-Gb sequence passed all the NIST statistical tests indicating it is random with 99% confidence.

The maximum bit-rate supported by this RNG depends on the turn-“on” and turn-“off” dynamics of the OPO. At the end of each clock cycle, the intracavity field must decay to the quantum noise level [11], or the residual field from the previous state will seed oscillation of the next state, and randomness will be lost. In the design presented here, the clock speed is slow enough (and OPO “on”-time long enough) that oscillation build to a steady-state level. In this case, the clock rate is limited by the time it takes for the intensity to decay below noise, which is 10 to 20 times longer than the $1/e$ cavity decay time when the OPO is pumped well over threshold and allowed to reach steady state. Therefore, the RNG speed is limited by the cavity decay time, and faster bit rates, in the Gbps range are expected to be achievable using pumps with higher

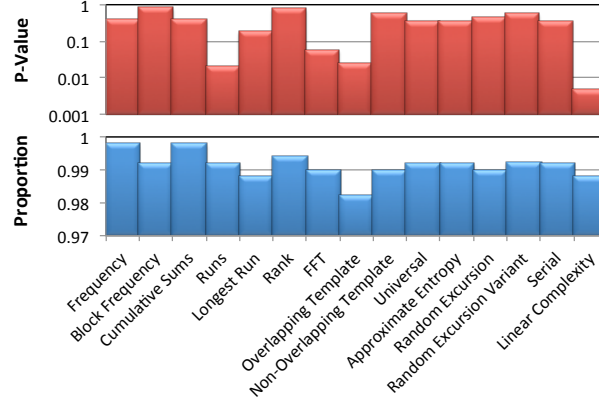


Figure 4: Summary of the results of the NIST statistical tests [19] on a sequence of 1 billion bits. The sequence is chopped into 500 shorter sequences and each test is performed on all sequences. Horizontal axes shows the name of the tests, $P-Value$ is the result of χ^2 distribution evaluation for all short sequences, and $Proportion$ is the proportion of the short sequences passed each test with a significance level of 0.01. The final decision on if the whole sequence has passed a test is made based on these criteria: $P-Value > 0.0001$ and $Proportion > 0.976$ [19], which are satisfied for all the tests.

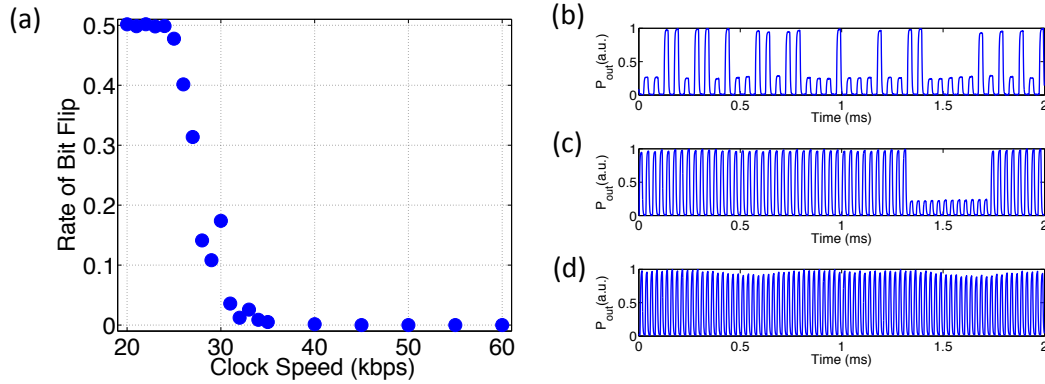


Figure 5: a) Dependence of the randomness on the clock speed; for each clock speed a sequence of 100 kb is recorded, and the rate of bit flip is calculated by counting the number of changes in the bit value and dividing it to the sequence length, for a random sequence the rate of bit flip is close to 0.5 and for a single-value sequence it is zero; The transition from random to non-random output occurred around 25 kbps which is close to the estimated value of 30 kbps taking into account the experiment parameters. This value can be increased by decreasing the overall pump power and approaching the threshold. To record the 1 Gb of data, the pump power was reduced so that the randomness would not break until 200 kbps (the measurement limit). b, c, d) a sample of the output sequence when clock speed is b) 20 kbps, c) 30 kbps, and d) 40 kbps.

repetition rates, and shorter OPO cavities [20, 21].

However, one can operate the OPO closer to threshold, where the build-up time is longer than the decay time. In this case, the oscillation will not necessarily reach steady-state, but relative phase may still be measured with a sufficiently sensitive detector to establish the bit value, decoupling maximum RNG speed from the cavity decay time. A potential extreme case is eliminating the cavity and having a single pass parametric down conversion with a speed as high as the repetition rate but requiring either a sensitive detection system or a relatively high peak power. It is even possible to design a similar RNG with a c.w. pump to eliminate the repetition rate limit.

We exploit the OPO dynamics discussed above to verify that the randomness is due to the phase of photons initiating the oscillation. As mentioned before, our RNG operates in the regime where build-up is much faster than decay. This is due to the low ($\sim 23\%$) modulation depth of the AOM that biases the pump only slightly below threshold during the “off” phase of the clock, resulting in a much longer decay time than if the OPO were un-pumped. This makes it easy to observe the transition to a fixed-state, ‘latched’ oscillation, when at faster clock rates the turn “on” edge arrives while many photons remain in the cavity. Figure 5-(a) shows how the randomness – measured here by the rate of bit flip in a 100-kb long sequence – breaks as a function of clock speed. Figure 5-(b),(c),(d) illustrate output samples for three points on this curve. This experiment shows that when an intracavity phase reference exists – in the form of residual photons from the previous clock cycle – the randomness of the sequence breaks and the influence of classical noise sources is negligible.

In summary, we demonstrated a novel technique for all-optical quantum RNGs based on the randomness in spontaneous parametric down conversion by measuring the above-threshold phase of oscillation in a degenerate OPO. The twin system, made of two identical OPOs sharing the same cavity, facilitates the phase state measurement. Stable operation is achieved using a free running commercially available mode-locked fiber laser. Unlike many other quantum RNGs, this system enables quantum random number generation with no need for electronic or computer post processing on the generated bit sequence, and has the potential of extremely fast operation. Implementation of an OPO-based quantum RNGs is not limited to second-order nonlinear materials and free space elements as presented here; one can extend this approach to on-chip χ^3 OPOs [22]– [24] where CMOS compatibility can open new possibilities for new generation of RNGs for future communication and computational systems. Combined with micro- and nano resonators, this technique paves the way for high-speed all-optical quantum RNGs with multi Gigabit per second rates.

Acknowledgements

The authors would like to thank S. E. Harris, Y. Yamamoto, M. M. Fejer, C. R. Phillips, J. S. Pelc, C. W. Rudy, and O. Crisafulli for invaluable discussions, and K. Urbanek for experimental support.

1 Methods

1.1 Experimental Setup

The OPO is pumped by a 1560-nm mode-locked Er-fiber laser (Menlo Systems C-fiber, 100 MHz, 70 fs, 300 mW) where beam is conditioned by a mode-matching telescope for efficient pumping of the OPO. The resonator is a 6-m ring cavity corresponding to twice the spacing between the pump laser pulses. The cavity optics comprise one pair of concave mirrors with ROC=50 mm (M_2 and M_3), and six flat mirrors (twice folded bow tie), five of which are gold coated with approximately 99% reflection (only one is depicted in schematic of Fig. 2: M_4). A single dielectric mirror (M_1) is used to introduce the pump, which has 90%

transmission for the pump and more than 99% reflection in the 2.8 - 4 μm . This mirror has a ‘chirped’ design of dielectric layers to compensate the dispersion of the nonlinear crystal.

Broadband gain centered around 3.1 μm is provided by 1-mm long MgO-doped periodically poled lithium niobate (MgO:PPLN) crystal. The poling period is 34.8 μm for broadband type-0 (e=e+e) phase matching at a temperature of 32°C. The crystal is cut such that the mid-IR beam propagates perpendicular to the poling domains when the beam enters at the Brewster angle. The beam waist for signal beam in the crystal is $\sim 10 \mu\text{m}$. The mirrors M_2 and M_3 are set to 5-degree angle of incidence to compensate the astigmatism caused by the Brewster angled crystal and allow stable resonances in the 6-m long cavity. The output is extracted with a pellicle beam splitter (OC) having $\sim 8\%$ reflection over a broad bandwidth. The filters are AR coated Ge substrates to block the pump and allow the mid-IR signal go through.

Oscillation occurs when signal/idler waves are brought into degenerate resonance by fine-tuning the cavity length with the piezo stage of M_4 . Three of these resonances occur separated by $\sim 1.5 \mu\text{m}$ of roundtrip cavity length, corresponding to half of the signal central wavelength [16]. Continuous operation of the OPO is obtained by locking the cavity length to track the center of the strongest resonance using a dither-and-lock scheme [16]. The twin OPO starts oscillating at a pump average power of about 120 mW, and the maximum mid-IR output power is 4 mW.

1.2 Estimated Maximum Speed

The twin OPO operates in the regime where the build up time is faster than the decay time. Therefore, for quantum RNG outcome the turn off time should be long enough to allow the intracavity power to decay from the steady state level, that is about 1 W, to the quantum noise level, i.e. one photon per mode ($P_{\text{noise}} = h\nu\Delta\nu$ [15]), which is about 1 μW . Here $h\nu$ is the photon energy at the central signal wavelength of 3.1 μm , and $\Delta\nu$ is the OPO bandwidth at 3-dB level, estimated to be $\sim 10 \text{ THz}$ (Fig. 3-a). The intensity decay time of the OPO can be estimated using:

$$\tau_{\text{off}} = \frac{T}{2\delta_E - 2\delta_E \sqrt{\frac{P_{\text{off}}}{P_{\text{th}}}}},$$

where δ_E is the electric-field fractional round-trip loss, P_{th} is the pump power at threshold, P_{off} is the pump power at the “off” state, and T is the cavity roundtrip time. In the presence of the AOM, the OPO threshold measured before M_1 is increased to 190 mW because of pulse broadening in the AOM. The pump power at the off state is 168 mW, and intracavity power loss ($2\delta_E$) is estimated to be 0.27 resulting in the 1/e intensity decay time of 1.2 μs . Hence the minimum turn-off time required for decaying from steady state power to quantum noise level is about 17 μs corresponding to a maximum clock speed of $\sim 30 \text{ kbps}$.

References

- [1] S. Pironio, A. Acin, S. Massar, A. B. de la Giroday, D. N. Matsukevich, P. Maunz, S. Olmschenk, D. Hayes, L. Luo, T. A. Manning, C. Monroe, “Random numbers certified by Bells theorem,” *Nature* 464, 1021 – 1024 (2010).
- [2] M. Fiorentino, C. Santori, S. M. Spillane, R. G. Beausoleil, W. J. Munro, “Secure self-calibrating quantum random-bit generator,” *Phys. Rev. A* 75, 032334 (2007).
- [3] C. Gabriel, C. Wittmann, D. Sych, R. Dong, W. Maurer, U. L. Andersen, C. Marquardt, G. Leuchs, “A generator for unique quantum random numbers based on vacuum states,” *Nature Photonics* 4, 711 – 715 (2010).

- [4] M. Wahl, M. Leifgen, M. Berlin, T. Rhlicke, H. Rahn, O. Benson, “An ultrafast quantum random number generator with provably bounded output bias based on photon arrival time measurements,” *Appl. Phys. Lett.* 98, 171105 (2011).
- [5] M. Ren, E. Wu, Y. Liang, Y. Jian, G. Wu, H. Zeng, “Quantum random-number generator based on a photon-number-resolving detector,” *Phys. Rev. A* 83, 023820 (2011).
- [6] M. Jofre, M. Curty, F. Steinlechner, G. Anzolin, J. P. Torres, M. W. Mitchell, V. Pruneri, “True random numbers from amplified quantum vacuum,” *Opt. Express* 19, 20665–20672 (2011)
- [7] B. Qi, Y. Chi, H. Lo, Li Qian, “High-speed quantum random number generation by measuring phase noise of a single-mode laser,” *Opt. Lett.* 35, 312–314 (2010).
- [8] P. J. Bustard, D. Moffatt, R. Lausten, G. Wu, I. A. Walmsley, B. J. Sussman, “Quantum random bit generation using stimulated Raman scattering,” *Opt. Express* 19, 25173–25180 (2011).
- [9] L. Wu, H. J. Kimble, J. L. Hall, H. Wu, “Generation of Squeezed States by Parametric Down Conversion,” *Phys. Rev. Lett.* 57, 2520–2523 (1986).
- [10] Y. H. Shih, C. O. Alley, “New Type of Einstein-Podolsky-Rosen-Bohm Experiment Using Pairs of Light Quanta Produced by Optical Parametric Down Conversion,” *Phys. Rev. Lett.* 61, 2921-2924 (1988).
- [11] W. H. Louisell, A. Yariv, A. E. Siegman, “Quantum Fluctuations and Noise in Parametric Processes I,” *Phys. Rev.* 124, 1646 (1961).
- [12] S. E. Harris, M. K. Oshman, R. L. Byer, “Observation of Tunable Optical Parametric Fluorescence,” *Phys. Rev. Lett.* 18, 732–734 (1967).
- [13] C. D. Nabors, S. T. Yang, T. Day, R. L. Byer, “Coherence properties of a doubly-resonant monolithic optical parametric oscillator,” *J. Opt. Soc. Am. B* 7, 815 – 820 (1990).
- [14] L. E. Myers, R. C. Eckardt, M. M. Fejer, R. L. Byer, W. R. Bosenberg, J. W. Pierce, “Quasi-phase-matched optical parametric oscillators in bulk periodically poled LiNbO₃,” *JOSA B*, v. 12, n. 11, pp. 2102-2116 (1995).
- [15] A. Yariv, P. Yeh, “Photonics,” Sixth Ed., Oxford University Press, 2007.
- [16] N. Leindecker, A. Marandi, R. L. Byer, K. L. Vodopyanov, “Broadband Degenerate OPO for Mid-Infrared Frequency Comb Generation,” *Opt. Express* 19, 6296–6302 (2011).
- [17] S. T. Wong, K. L. Vodopyanov, R. L. Byer, “Self-phase-locked divide-by-2 optical parametric oscillator as a broadband frequency comb source,” *J. Opt. Soc. Am. B* 27, 876–882 , (2010).
- [18] A. Marandi, N. Leindecker, V. Pervak, R. L. Byer, K. Vodopyanov, “Coherence properties of a broadband femtosecond mid-IR optical parametric oscillator operating at degeneracy,” *Opt. Express* 20, 72557262 (2012).
- [19] A. Rukhin, J. Soto, J. Nechvatal, M. Smid, E. Barker, S. Leigh, M. Levenson, M. Van- gel, D. Banks, A. Heckert, J. Dray, S. Vo, “A statistical test suite for random and pseudorandom number generators for cryptographic applications,” NIST special publication 800-22, Rev. 1-a, NIST, Gaithersburg, Maryland, USA, (2010).

- [20] S. Lecomte, R. Paschotta, S. Pawlik, B. Schmidt, K. Furusawa, A. Malinowski, D. J. Richardson, U. Keller, "Synchronously Pumped Optical Parametric Oscillator With a Repetition Rate of 81.8 GHz," *IEEE Phot. Technol. Lett.* v. 17, n. 2, pp 483-485 (2005).
- [21] J. U. Furst, D. V. Strekalov, D. Elser, A. Aiello, U. L. Andersen, Ch. Marquardt, G. Leuchs, "Quantum Light from a Whispering-Gallery-Mode Disk Resonator," *Phys. Rev. Lett.* 106, 113901 (2011).
- [22] J. S. Levy, A. Gondarenko, M. A. Foster, A. C. Turner-Foster, A. L. Gaeta, M. Lipson, "CMOS-compatible multiple-wavelength oscillator for on-chip optical interconnects," *Nature Photonics* 4, 37 - 40 (2010).
- [23] L. Razzari, D. Duchesne, M. Ferrera, R. Morandotti, S. Chu, B. E. Little, D. J. Moss, "CMOS-compatible integrated optical hyper-parametric oscillator," *Nature Photonics* 4, 41 - 45 (2010).
- [24] X. Liu, R. M. Osgood, Y. A. Vlasov, W. M. J. Green, "Mid-infrared optical parametric amplifier using silicon nanophotonic waveguides," *Nature Photonics* 4, 557 - 560 (2010).